Efficient Quantum Algorithm for the Hidden Parabola Problem

Thomas Decker* and Pawel Wocjan†

March 20, 2007

Abstract

We introduce the Hidden Polynomial Function Graph Problem as a natural generalization of the abelian Hidden Subgroup Problem (HSP) over groups of the form $\mathbb{Z}_p \times \mathbb{Z}_p$, where the hidden subgroups are generated by $(1, a)$ for different $a \in \mathbb{Z}_p$. These subgroups and their cosets correspond to graphs of linear functions on $\mathbb{Z}_p$. For the Hidden Polynomial Function Graph Problem the functions are not restricted to be linear but can also be polynomial functions of degree $n \geq 2$.

Analogously to the HSP, for a fixed degree n the Hidden Polynomial Function Graph Problem is hard on a classical computer as its query complexity is polynomial in p. To solve this problem on a quantum computer in time polylogarithmic in p, we first reduce it to a quantum state identification problem and then we use the pretty good measurement (PGM) approach to construct measurements for distinguishing the states.

We relate the success probability and implementation of the PGM to a certain classical problem involving polynomial equations. We present an efficient quantum algorithm for the case of hidden parabola by establishing that the success probability of the PGM is lower bounded by a constant and that the PGM can be implemented efficiently.

1 Introduction

Quantum algorithms allow us to solve certain problems more efficiently than any or the currently best known classical algorithms. However, the exact extent of the computational advantage of quantum computers over classical computers is not well understood.

Shor's algorithm for factoring integers and calculating discrete logarithms [17] is one of the most important and well known examples of quantum computational speedups.

*Department of Computer Science & Engineering, University of Washington, Seattle, WA 98195, USA. Electronic address: decker@ira.uka.de

†School of Electrical Engineering and Computer Science, University of Central Florida, Orlando, FL 32816, USA. Electronic address: wocjan@cs.ucf.edu

This algorithm and other fast quantum algorithms for number-theoretic problems [10, 11, 16] essentially rely on the efficient solution of an abelian hidden subgroup problem (HSP) [4].

This has naturally raised the questions of what interesting problems can be reduced to the nonabelian HSP and of whether the general nonabelian HSP can also be solved efficiently on a quantum computer. It is known that an efficient quantum algorithm for the dihedral HSP would give rise to efficient quantum algorithms for certain lattice problems [15], and an efficient quantum algorithm for the symmetric group would give rise to an efficient quantum algorithm for the graph isomorphism problem [6]. For these reasons, the nonabelian HSP has been one of the most extensively studied approaches for designing quantum algorithms. Despite the fact that efficient algorithms have been developed for more and more special cases of this problem (see, for example, [14] and the references therein), the two cases with important algorithmic applications, the HSPs over the dihedral group and the symmetric group have withstood all attempts so far. Moreover, there is evidence that the nonabelian HSP might be hard for some groups such as the symmetric group [12].

Therefore, it is important to explore new classes of problems which could be tractable on quantum computers but which require exponential resources on classical computers. Examples of such problems encompass several different Hidden Shift Problems which are closely related to the abelian HSP. Many instances of these problems can be solved efficiently on a quantum computer [3, 7]. Another idea going beyond the abelian HSP is to consider hidden non-linear structures [5]. In this context, we define a new black-box problem, called the Hidden Polynomial Function Graph Problem, and present efficient quantum algorithms for special cases.

The Hidden Polynomial Function Graph Problem is a natural generalization of the abelian HSP over groups of the special form $G := \mathbb{Z}_p \times \mathbb{Z}_p$, where the hidden subgroups are generated by $(1, q_1)$ for $q_1 \in \mathbb{Z}_p$. Therefore, the hidden subgroups H_Q and their cosets $H_{Q,z}$ are given by

$$H_Q := \{(x, Q(x)) : x \in \mathbb{Z}_p\} \quad \text{and} \quad H_{Q,z} := \{(x, Q(x) + z) : x \in \mathbb{Z}_p\},$$

where $z \in \mathbb{Z}_p$ and Q runs over all linear polynomials of the form $Q(X) := q_1 X$. In the Hidden Polynomial Function Graph Problem the polynomials $Q(X)$ are no longer restricted to be linear but can also be of degree $n \geq 2$, i.e., we have $Q(X) = \sum_{i=1}^{n} q_i X^i$. The subgroups are generalized to graphs of polynomial functions going through the origin $(0, 0)$ and their cosets to function graphs which are translated vertically.

Several other generalizations of the abelian HSP have been presented in [5]. We describe later how the Hidden Polynomial Function Graph Problem is related to the Hidden Polynomial Problem which was defined in that work.

Analogously to many interesting HSP, our problem is classically hard as its classical query complexity is polynomial in the field size p. Our approach to solve this problem on a quantum computer is to generalize standard techniques for the HSP. First, we reduce the Hidden Polynomial Function Graph Problem to a quantum state identification problem. Second, we use the pretty good measurement (PGM) approach [1] to systematically construct measurements for distinguishing the quantum states. Third, we relate the success probability and implementation of the PGM to a certain classical problem involving polynomial equations. We present an efficient quantum algorithm for the case of quadratic polynomials by establishing that the success probability of the PGM is lower bounded by a constant and that the measurement can be implemented efficiently.

The paper is organized as follows: In Section 2 we define the Hidden Polynomial Function Graph Problem and compare it to the Hidden Polynomial Problem studied in [5]. In Section 3 we adapt the standard approach for HSPs to the new problem. In Section 4 we discuss the properties of the states we obtain with the modified standard approach. In Section 5 we construct a measurement to distinguish these states. In Section 6 we discuss the case of quadratic functions thoroughly and show that an efficient solution for this special case exists. In Section 7 we conclude and discuss possible objectives for further research.

2 Hidden Polynomial Function Graph Problem

We define the Hidden Polynomial Function Graph Problem as a generalization of particular abelian HSPs. Whereas in the case of a HSP we want to identify a subgroup hidden by a black-box function, in our case we rather want to efficiently identify a polynomial that is hidden by a black-box function.

Definition (Hidden Polynomial Function Graph Problem):
Let $Q(X) = \sum_{i=1}^{n} q_i X^i \in \mathbb{Z}_p[X]$ be an arbitrary polynomial of degree n whose constant term is equal to zero. Let $F : \mathbb{Z}_p^2 \to \mathbb{Z}_p$ be a black-box function hiding the polynomial Q in the following sense:

$$F(x,y) = F(u,v)$$

iff there is an element $z \in \mathbb{Z}_p$ such that

$$y = Q(x) + z \text{ and } v = Q(u) + z\,,$$

i.e., the function F is constant on $\{(x, Q(x) + z) : x \in \mathbb{Z}_p\}$ and distinct for different values of z.

The Hidden Polynomial Function Graph Problem is to identify the polynomial Q if only the black-box function F is given. An algorithm for polynomials with constant degree n is efficient if its running time is polylogarithmic in p.

An alternative definition of the function F is given by

$$F(x,y) := \pi(y - Q(x))$$

where π is an unknown and irrelevant bijection $\pi : \mathbb{Z}_p \to \mathbb{Z}_p$ which permutes the elements of $\mathbb{Z}_p$ arbitrarily.

The Hidden Polynomial Function Graph Problem is hard to solve with a classical computer as its query complexity is polynomial in p. This is because at least n different points

$$(x_1, y_1), \ldots, (x_n, y_n) \quad \text{with} \quad F(x_1, y_1) = \ldots = F(x_n, y_n)$$

are required in order to determine the hidden polynomial Q of degree n. The probability of obtaining such n-fold collision is smaller than the probability of obtaining a 2-collision. The probability of the latter is $1/p$. In contrast, there is an efficient quantum algorithm for quadratic polynomials $Q(X) = q_2X^2 + q_1X$.

The Hidden Polynomial Function Graph Problem is related to the Hidden Polynomial Problem defined in [5]. The Hidden Polynomial Problem for univariate polynomials can be equivalently reformulated as follows. The black-box function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is given by $f(x) = \sigma(Q(x))$, where σ is an arbitrary permutation of $\mathbb{Z}_p$ and $Q(X)$ is the hidden polynomial. It is readily seen that the black-boxes f can be obtained from the black-boxes F by querying F only at points of the form $(x, 0)$. For this reason the black-boxes F offer more flexibility in designing quantum algorithms. We are able to design an efficient quantum algorithm for the black-boxes F hiding quadratic polynomials, whereas no algorithms are known for the black-boxes f.

3 Standard Approach

Most quantum algorithms for HSPs are based on the standard approach. Therefore, this method can be seen as a natural way to approach the Hidden Polynomial Function Graph Problem. This leads to the following algorithm:

- Prepare an equally weighted superposition of all $(x, y) \in \mathbb{Z}_p^2$ and initialize the register for the results. Evaluate the black-box function F. The corresponding state transition is

$$\frac{1}{p}\sum_{x,y\in\mathbb{Z}_p}|x\rangle|y\rangle|0\rangle \mapsto \frac{1}{p}\sum_{x,y\in\mathbb{Z}_p}|x\rangle|y\rangle|F(x,y)\rangle$$

- Measure and discard the third register. Assume we have obtained the measurement result $\pi(z)$. Then the state on the first and second register is

$$\rho_{Q,z} := |\phi_{Q,z}\rangle\langle\phi_{Q,z}| \quad \text{with} \quad |\phi_{Q,z}\rangle := \frac{1}{\sqrt{p}}\sum_{b\in\mathbb{Z}_p}|b\rangle|Q(b)+z\rangle\,,$$

  where Q is the unknown polynomial hidden by F and z is uniformly at random. The corresponding density matrix is

$$\rho_Q := \frac{1}{p}\sum_{z\in\mathbb{Z}_p}|\phi_{Q,z}\rangle\langle\phi_{Q,z}|\,. \tag{1}$$

  We refer to the states ρ_Q as *polynomial function states*.

This variant of the standard approach to HSP also reduces the Hidden Polynomial Function Graph Problem to a state distinguishing problem: Given a polynomial function state ρ_Q with unknown Q decide which state it is. In Sec. 6 we show that an efficient identification of ρ_Q is possible at least for quadratic polynomials. The basis of this solution is the structure of the states which can be used to construct and implement a measurement which allows us to distinguish among the quantum states with high success probability.

4 Structure of Polynomial Function States

The starting point of our analysis are the states $\rho_{Q,z}$ which can be written as

$$\rho_{Q,z} = \frac{1}{p} \sum_{b,c\in\mathbb{Z}_p} |b\rangle\langle c| \otimes |Q(b)+z\rangle\langle Q(c)+z| \,.$$

By averaging these states over z we obtain the density matrix ρ_Q of Eq. (1). To obtain a compact notation we introduce the cyclic shift

$$S_p|x\rangle := |x+1 \bmod p\rangle$$

for which we obtain the equation

$$\sum_{z\in\mathbb{Z}_p} |b+z\rangle\langle c+z| = S_p^{b-c}\,.$$

This directly leads to

$$\rho_Q := \frac{1}{p^2} \sum_{b,c\in\mathbb{Z}_p} |b\rangle\langle c| \otimes S_p^{Q(b)-Q(c)}\,.$$

Now we use the fact that the shift operator S_p and its powers can be diagonalized simultaneously with the Fourier matrix

$$F_p := \frac{1}{\sqrt{p}} \sum_{k,\ell\in\mathbb{Z}_p} \omega_p^{k\ell} |k\rangle\langle \ell|\,,$$

i.e., we have

$$F_p S_p^k F_p^\dagger = \sum_{u\in\mathbb{Z}_p} \omega_p^{uk} |u\rangle\langle u|\,,$$

where $\omega_p := e^{2\pi i/p}$ is a pth root of unity. Hence, the Fourier transformed density matrices have the block diagonal form

$$\tilde{\rho}_Q := (I_p \otimes F_p)\rho_Q(I_p \otimes F_p^\dagger) = \frac{1}{p^2} \sum_{b,c,x\in\mathbb{Z}_p} \omega_p^{[Q(b)-Q(c)]x} |b,x\rangle\langle c,x|$$

in the Fourier basis where I_p denotes the identity matrix of size p and where we write $|b,x\rangle := |b\rangle \otimes |x\rangle$.

By repeating the standard approach k times for the same function F, we obtain the density matrix $\tilde{\rho}_Q^{\otimes k}$. After rearranging the registers we can write

$$\begin{aligned}
\tilde{\rho}_Q^{\otimes k} &= \frac{1}{p^{2k}} \sum_{b,c,x\in\mathbb{Z}_p^k} \omega_p^{\sum_{j=1}^k [Q(b_j)-Q(c_j)]x_j} |b,x\rangle\langle c,x| \\
&= \frac{1}{p^{2k}} \sum_{b,c,x\in\mathbb{Z}_p^k} \omega_p^{\sum_{j=1}^k [\sum_{i=1}^n q_i(b_j^i - c_j^i)]x_j} |b,x\rangle\langle c,x| \\
&= \frac{1}{p^{2k}} \sum_{b,c,x\in\mathbb{Z}_p^k} \omega_p^{\sum_{i=1}^n q_i[\sum_{j=1}^k (b_j^i - c_j^i)x_j]} |b,x\rangle\langle c,x| \\
&= \frac{1}{p^{2k}} \sum_{b,c,x\in\mathbb{Z}_p^k} \omega_p^{\langle q|\Phi^{(n)}(b)-\Phi^{(n)}(c)|x\rangle} |b,x\rangle\langle c,x|\,,
\end{aligned}$$

where $\langle q|$, $\Phi^{(n)}(b)$, $\Phi^{(n)}(c)$, and $|x\rangle$ are defined as follows:

- $\langle q| = (q_1, q_2, \ldots, q_n) \in \mathbb{Z}_p^{1\times n}$ is the row vector whose entries are the coefficients of the hidden polynomial $Q(X) = \sum_{i=1}^{n} q_i X^i$,
- $\Phi^{(n)}(b)$ is the $n \times k$ matrix

$$\Phi^{(n)}(b) = \sum_{i=1}^{n}\sum_{j=1}^{k} b_j^i |i\rangle\langle j| = \begin{pmatrix} b_1 & b_2 & \cdots & b_k \\ b_1^2 & b_2^2 & \cdots & b_k^2 \\ \vdots & \vdots & & \vdots \\ b_1^n & b_2^n & \cdots & b_k^n \end{pmatrix},$$

- $\Phi^{(n)}(c)$ is the $n \times k$ matrix

$$\sum_{i=1}^{n}\sum_{j=1}^{k} c_j^i |i\rangle\langle j| = \begin{pmatrix} c_1 & c_2 & \cdots & c_k \\ c_1^2 & c_2^2 & \cdots & c_k^2 \\ \vdots & \vdots & & \vdots \\ c_1^n & c_2^n & \cdots & c_k^n \end{pmatrix},$$

- $|x\rangle := (x_1, \ldots, x_k)^T \in \mathbb{Z}_p^{k\times 1}$ is the column vector whose entries are the entries of x.

We use the ideas of [1] to simplify the further constructions with the states $\tilde{\rho}_Q^{\otimes k}$. Let $w = (w_1, \ldots, w_n) \in \mathbb{Z}_p^n$ and $|w\rangle \in \mathbb{Z}_p^{n\times 1}$ be the corresponding column vector. Consider the matrix problem to determine all $b \in \mathbb{Z}_p^k$ for given $x \in \mathbb{Z}_p^k$ and $w \in \mathbb{Z}_p^n$ such that $\Phi^{(n)}(b)|x\rangle = |w\rangle$, i.e.,

$$\begin{pmatrix} b_1 & b_2 & \cdots & b_k \\ b_1^2 & b_2^2 & \cdots & b_k^2 \\ \vdots & \vdots & & \vdots \\ b_1^n & b_2^n & \cdots & b_k^n \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix} = \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix}$$

The set of solutions to this matrix problem, i.e., to these polynomial equations, defines an algebraic variety. We denote this set by

$$S_w^x := \{b \in \mathbb{Z}_p^k \,|\, \Phi^{(n)}(b)|x\rangle = |w\rangle\}$$

and its cardinality by

$$\eta_w^x := |S_w^x|\,.$$

We also define the quantum states $|S_w^x\rangle$ to be the equally weighted superposition of all solutions

$$|S_w^x\rangle := \frac{1}{\sqrt{\eta_w^x}} \sum_{b\in S_w^x} |b\rangle$$

if $\eta_w^x > 0$ and $|S_w^x\rangle$ to be the zero vector otherwise. Using this notation, we can express the state $\tilde{\rho}_Q^{\otimes k}$ as

$$\tilde{\rho}_Q^{\otimes k} := \frac{1}{p^{2k}} \sum_{x\in\mathbb{Z}_p^k} \sum_{w,v\in\mathbb{Z}_p^n} \omega_p^{\langle q|w\rangle - \langle q|v\rangle} \sqrt{\eta_w^x \eta_v^x} |S_w^x, x\rangle\langle S_v^x, x|\,.$$

This form is very useful for the construction of the pretty good measurement which we will use for distinguishing the states $\rho_Q^{\otimes k}$ for different polynomials Q and for computing the success probability.

5 The Pretty Good Measurement

A simple yet very useful measurement for distinguishing the states of a given ensemble is the pretty good measurement (PGM) [13] (also known as the square root measurement or least squares measurement [8]). For example, the PGM is the optimal measurement for distinguishing the hidden subgroup states arising in the HSP over the dihedral group [1]. Moreover, it provides the basis for the efficient quantum algorithms for HSPs over semidirect product groups [2].

In our situation, the PGM for the states $\tilde{\rho}_Q^{\otimes k}$ consists of the operators

$$E_Q := \frac{1}{p^n}\sqrt{\tilde{\rho}^-}\,\tilde{\rho}_Q^{\otimes k}\sqrt{\tilde{\rho}^-}$$

where $\tilde{\rho}^-$ denotes the pseudo inverse of the density matrix

$$\tilde{\rho} := \frac{1}{p^n}\sum_Q \tilde{\rho}_Q^{\otimes k}$$

corresponding to the polynomial function states $\tilde{\rho}_Q^{\otimes k}$, where Q runs over all polynomials of degree n without constant term. Explicitly, we obtain

$$\tilde{\rho} = \frac{1}{p^{2k}}\sum_{x\in\mathbb{Z}_p^k}\sum_{w\in\mathbb{Z}_p^n}\eta_w^x|S_w^x,x\rangle\langle S_w^x,x|$$

since the equation

$$\sum_{q\in\mathbb{Z}_p^n}\omega_p^{\langle q|w\rangle-\langle q|v\rangle} = p^n\delta_{w,v}$$

holds for the Kronecker $\delta_{w,v}$. The square root of the pseudo inverse of $\tilde{\rho}$ turns out to be

$$\sqrt{\tilde{\rho}^-} = p^k\sum_{x\in\mathbb{Z}_p^k}\sum_{w\in\mathbb{Z}_p^n}\sqrt{\frac{1}{\eta_w^x}}|S_w^x,x\rangle\langle S_w^x,x|\,.$$

Therefore, we obtain the PGM operators

$$E_Q := \frac{1}{p^n}\sum_{x\in\mathbb{Z}_p^k}\sum_{w,v\in\mathbb{Z}_p^n}\omega^{\langle q|w\rangle-\langle q|v\rangle}|S_w^x,x\rangle\langle S_v^x,x| \tag{2}$$

where $q\in\mathbb{Z}_p^n$ corresponds to Q. Since for a POVM on a p^2-dimensional system with positive-semidefinite operators E_i the equation $\sum_i E_i = I_{p^2}$ must hold, we need additional operators for the PGM of the polynomial states if $\tilde{\rho}$ does not have full rank. In the following we can neglect these operators for the computations of probabilities since these additional operators are orthogonal to all $\tilde{\rho}_Q^{\otimes k}$. Simple computations show that the PGM with the operators E_Q of Eq. (2) lead to the success probability

$$\mathrm{tr}(\tilde{\rho}_Q^{\otimes k} E_Q) = \frac{1}{p^{2k+n}} \sum_{x \in \mathbb{Z}_p^k} \left(\sum_{w \in \mathbb{Z}_p^n} \sqrt{\eta_w^x} \right)^2 . \tag{3}$$

A natural way to implement the PGM follows from the block diagonal structure of the operators E_Q in Eq. (2). The operators can be written as

$$E_Q = \sum_{x \in \mathbb{Z}_p^k} E_Q^x \otimes |x\rangle\langle x| \quad \text{with} \quad E_Q^x := \frac{1}{p^n} \sum_{w,v \in \mathbb{Z}_p^n} \omega_p^{\langle q|w\rangle - \langle q|v\rangle} |S_w^x\rangle\langle S_v^x| \,.$$

This structure suggests that we use an implementation scheme with two stages. In the first stage we apply an orthogonal measurement on the second tensor component of the system in the standard basis. Assume that the measurement result is $x \in \mathbb{Z}_p^k$. Depending on this result we have to implement the POVM with the operators E_Q^x on the remaining register of the system.

To this end, we embed everything into a larger Hilbert space $(\mathbb{C}^p)^{\otimes m} \otimes (\mathbb{C}^p)^{\otimes m} \otimes \mathbb{C}^2$, where $m := \max\{k, n\}$. The first tensor component contains the quantum states $|w\rangle$ (where $w \in \mathbb{Z}_p^n$) and $|S_w^x\rangle$ (which are a superpositions of certain vectors $|b\rangle$, where $b \in \mathbb{Z}_p^k$). The second tensor component stores the quantum states $|x\rangle$ (where $x \in \mathbb{Z}_p^k$). The third register is used to indicate if $\eta_w^x = 0$. All tuples $w \in \mathbb{Z}_p^n$ and $b, x \in \mathbb{Z}_p^k$ are padded suitably with zeros to have length m.

To implement the POVM we consider the transformation V defined by

$$|w, x, 0\rangle \mapsto \begin{cases} |S_w^x, x, 0\rangle & \eta_w^x > 0 \\ |w, x, 1\rangle & \eta_w^x = 0 \end{cases} \tag{4}$$

for all $w \in \mathbb{Z}_p^n$ and all $x \in \mathbb{Z}_p^k$. The transformation V is defined to act as the identity on the subspace spanned by all basis vectors not covered on the left hand side of Eq. (4). It is obvious that V can be implemented efficiently provided that we can create the superpositions $|S_w^x\rangle$ for all w and x. The POVM defined by the operators E_Q^x can be realized by first appending a qubit with state $|0\rangle\langle 0|$ and applying $V^\dagger$ and then measuring in the Fourier basis. In the next section we show that there is an efficient preparation of these superpositions $|S_w^x\rangle$ for quadratic polynomials.

6 Hidden Parabola

We show that the standard approach of Sec. 3 and the PGM of Sec. 5 lead to an efficient algorithm for a hidden parabola defined by the quadratic polynomial $Q(X) = q_2 X^2 + q_1 X$. We show that for two copies of the polynomial function states the success probability is lower bounded by a constant. Additionally, we argue that the PGM can be implemented efficiently.

For a single copy of the polynomial function state ρ_Q, i.e., we have $k = 1$, it turns out that the PGM is the optimal measurement for distinguishing the states. However, for a single-copy measurement the success probability is only

$$\frac{1}{p} + O\left(\frac{1}{p^2}\right)$$

which does not leads to an efficient algorithm. In contrast, if we construct the PGM for two copies, i.e. $k = 2$, then we can show that the success probability of the PGM is lower bounded by a constant. This strongly resembles the situation for the Heisenberg-Weyl HSP, where a single copy is also not sufficient but the PGM of two copies lead to an efficient quantum algorithm [2].

For quadratic polynomials we have to consider the sets

$$S_{(w_1,w_2)}^{(x_1,x_2)} = \left\{(b_1, b_2) \in \mathbb{Z}_p^2 \mid \begin{pmatrix} b_1 & b_2 \\ b_1^2 & b_2^2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}\right\}.$$

We set $b = b_1$, $c = b_2$, $x = x_1$, $y = x_2$, $v = w_1$, and $w = w_2$ to avoid too many indices. Therefore, we have to find the set of solutions of the equations

$$bx + cy = v \quad \text{and} \quad b^2x + c^2y = w\,. \tag{5}$$

Depending on x and y which are determined by the orthogonal measurement in the first stage as well as by v and w the set of solutions can encompass 0, 1, 2, p or p^2 solutions. To derive a lower bound on the success probability of Eq. (3) it suffices to consider the $p^2 - 3p + 2$ cases where

$$x, y \neq 0 \quad \text{and} \quad x \neq -y\,.$$

In these cases the equations of (5) have the solutions (b_j, c_j) with

$$c_{1/2} := \frac{v}{x+y} \pm \frac{1}{x+y}\sqrt{D} \quad \text{and} \quad b_{1/2} = \frac{v}{x} - \frac{y}{x}c_{1/2}$$

provided that

$$D := \frac{x}{y}w((x+y) - v^2)$$

is a square in $\mathbb{Z}_p$. For each pair (x, y) there are $p(p+1)/2$ pairs (v, w) such that the resulting D is a square. In this case, there is at least one solution. Therefore, we have the following lower bound on the success probability

$$\frac{1}{d^6}\sum_{(x,y)}\left(\sum_{(v,w)}\sqrt{\eta_{(v,w)}^{(x,y)}}\right)^2 \geq \frac{1}{p^6}\left(p^2 - 3p + 2\right)\left(\frac{p(p+1)}{2}\right)^2 = \frac{1}{4} - O\left(\frac{1}{p}\right).$$

In the remaining part of this section we argue that the measurement can be implemented efficiently. Following the discussion of the end of Sec. 5 we only have to show that we can implement the transform of (4) efficiently. This means that we have to prepare the superposition of all solutions of equations (5). For $n = 2$ we can find the solutions of the $p^2 - 3p + 2$ considered cases with $O(\log(p))$ operations on a classical computer (see Cor. 14.16 in [9]). Since there are at most two solutions the superposition can be prepared efficiently. For completeness, we give the remaining cases with at least one solution (their overall probability is negligible):

- For $(x,y) = (0,0)$ we have the p^2 solutions (b,c) with arbitrary $b,c \in \mathbb{Z}_p$ for $w,v = 0$.
- For $(x,y) = (0,y)$ with $y \neq 0$ we have the p solutions $(b,c) = (b,0)$ with arbitrary $b \in \mathbb{Z}_p$ if $w = 0$. For $w,v \neq 0$ we have the p solutions $(b,c) = (b, v/y)$ with arbitrary $b \in \mathbb{Z}_p$ if $v^2 = wy$.
- For $(x,y) = (x,0)$ with $x \neq 0$ we have the p solutions $(b,c) = (0,c)$ with arbitrary $c \in \mathbb{Z}_p$ if $w,v = 0$. For $w,v \neq 0$ we have the p solutions $(b,c) = (v/x, c)$ with arbitrary $c \in \mathbb{Z}_p$ if $v^2 = wx$.
- For $(x,y) = (x,-x)$ with $x \neq 0$ we have the p solutions $(b,c) = (b,b)$ with arbitrary $b \in \mathbb{Z}_p$ for $w,v = 0$. For $v \neq 0$ we have the single solution

$$(b,c) = \left(\frac{wx + v^2}{2vx}, \frac{wx - v^2}{2vx} \right) .$$

In all cases, the solutions of Eqs. (5) can be computed easily and the corresponding superpositions can be created efficiently.

7 Conclusion and Outlook

We have introduced the Hidden Polynomial Function Graph Problem as a generalization of the abelian Hidden Subgroup Problem. We have shown that both the standard approach and the pretty good measurement approach for HSP can be successfully adapted. This approach leads to efficient quantum algorithms for quadratic polynomials over prime fields. A generalization of all the methods to non-prime fields $\mathbb{F}_d$ is straightforward. The Fourier transform over $\mathbb{Z}_p$ has to be replaced by the Fourier transform over $\mathbb{F}_d$ which can be implemented efficiently [7].

The central points of interest for future research are the generalization to polynomials over rings (admitting a Fourier transform), polynomials of higher degree, multivariate polynomials, and a broader class of functions. Moreover, it would be important to find real-life problems which could be reduced to our black-box problem and the problems defined in [5].

Acknowledgment

The authors acknowledge helpful discussions with D. Bacon and D. Janzing. TD was supported under ARO/DTO quantum algorithms grant number W911NSF-06-1-0379.

References

[1] D. Bacon, A. Childs, and W. van Dam, *Optimal measurements for the dihedral hidden subgroup problem*, Chicago Journal of Theoretical Computer Science, Article 2, 2006.

[2] D. Bacon, A. Childs, and W. van Dam, *From optimal measurements to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups*, Proc. of the 46th Symposium on Foundations of Computer Science, 2005, pp. 469-478.

[3] A. Childs and W. van Dam, *Quantum algorithm for a generalized hidden shift problem*, Proc. 18th ACM-SIAM Symposium on Discrete Algorithms, 2007, pp. 1225-1234.

[4] R. Boneh and R. Lipton, *Quantum cryptanalysis of hidden linear functions*, Proc. Advances in Cryptology, Lecture Notes in Computer Science **963**, 1995, pp. 424–437.

[5] A. Childs, L. Schulman, and U. Vazirani, *Quantum algorithms for hidden nonlinear structures*, Personal communication and talk given at the QIP Workshop 2007, Brisbane, Australia, January 30 – February 3, 2007.

[6] M. Ettinger and P. Hoyer, *A quantum observable for the graph isomorphism problem*, quant-ph/9901029.

[7] W. van Dam, S. Hallgren, L. Ip, *Quantum Algorithms for some Hidden Shift Problems*, SIAM Journal on Computing, Volume 36, Issue 3, pp. 763-778.

[8] Y. C. Eldar, A. Megretski, and G. C. Verghese, *Optimal detection of symmetric mixed quantum states*, IEEE Transactions on Information Theory **50**, no. 6, 2004, pp. 1198–1207.

[9] J. von zur Gathen, J. Gerhard: Modern Computer Algebra, Cambridge University Press, 2003.

[10] S. Hallgren, *Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem*, Proc. 34th ACM Symposium on Theory of Computing, 2002, pp. 653–658.

[11] S. Hallgren, *Fast quantum algorithms for computing the unit group and class group of a number field*, Proc. 37th ACM Symposium on Theory of Computing, 2005, pp. 468–474.

[12] S. Hallgren, C. Moore, M. Rötteler, A. Russell, and P. Sen, *Limitations of quantum coset states for graph isomorphism*, Proc. of 38th ACM Symposium on Theory of Computing, 2006, pp. 604 – 617.

[13] P. Hausladen and W. K. Wootters, *A 'pretty good' measurement for distinguishing quantum states*, Journal of Modern Optics **41**, no. 12, pp. 2385–2390.

[14] G. Ivanyos, L. Sanselme, and M. Santha, *Quantum algorithm for the hidden subgroup problem in extraspecial groups*, Proc. of 24th Annual Symposium on Theoretical Aspects of Computer Science, Lecture Notes in Computer Science **4393**, 2007, pp. 586–597.

[15] O. Regev, *Quantum computation and lattice problems*, Proc. 43rd Symposium on Foundations of Computer Science, 2002, pp. 520–529.

[16] A. Schmidt and U. Vollmer, *Polynomial time quantum algorithm for the computation of the unit group of a number field*, Proc. 37th ACM Symposium on Theory of Computing, 2005, pp. 475–480.

[17] P. W. Shor, *Polynomial-time algorithms for prime factorizations and discrete logarithms on a quantum computer*, SIAM Journal on Computing **26**, 1997, pp. 1484–1509.